MORNINGSTAR | DBRS

Commentary

Cyber Warfare Following Russia's Invasion of Ukraine Likely To Drive Up Claims for European and North American Insurers and Reinsurers

DBRS Morningstar
March 9, 2022

Marcos Alvarez
Senior Vice President, Head of Insurance
Global Financial Institutions Group
+34 662 976 415
marcos.alvarez@dbrsmorningstar.com

Elisabeth Rudman
Managing Director, Head of European FIG
Global Financial Institutions Group
+44 20 7855 6655
elisabeth.rudman@dbrsmorningstar.com

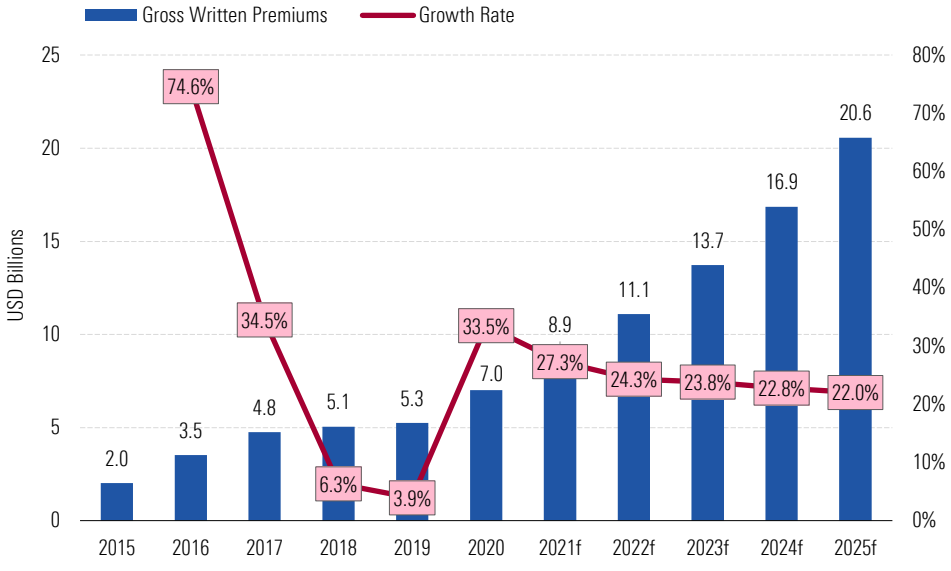
Key Highlights

- The Russia-Ukraine conflict has already increased the number of cyber incidents, but they mostly remain unsophisticated DDoS attacks.
- Although acts of war are typically excluded from cyber insurance policies, attribution remains a key challenge as most cyber warfare is typically not acknowledged by belligerent state actors.
- War exclusions in insurance policies have been updated in the past three years, but insurers and reinsurers are still trying to find a balance between the right coverage and managing accumulation risk.
- In DBRS Morningstar's view, claims should remain manageable for most insurance and reinsurance companies given updated exclusion clauses, reductions in limits, and product diversification.

Western governments have confirmed that the number of cyberattacks has materially increased following Russia's invasion of Ukraine and the recent tightening of economic and political sanctions on Russia. However, most cyber incidents so far have been relatively basic distributed denial-of-service (DDoS) attacks on both sides of the conflict. Cybersecurity experts and government agencies have voiced their concerns that state-sponsored and proxy attacks will become more sophisticated in the coming weeks, potentially affecting physical and financial infrastructure in most countries.

Although acts of war (declared or not) are typically excluded from cyber insurance policies, in DBRS Morningstar's view, the current conflict could potentially increase cyber-related insurance and reinsurance claims in Europe and North America, as attribution can be very difficult to determine in cyber incidents. In order to deny a cyber-related claim in this context, insurance and reinsurance companies will need to demonstrate beyond reasonable doubt that the claim in question is not related to a state-sponsored attack or performed by a group acting as a proxy of a belligerent government. DBRS Morningstar also expects a rise in litigation costs for the insurance industry as policyholders increasingly take denied claims to court. As shown in Exhibit 1, the global cyber insurance market has experienced tremendous growth since 2015 in response to more frequent and sophisticated cyberattacks, a trend that we expect to continue in the medium term with gross written premiums estimated to reach more than $20 billion by 2025.

Exhibit 1 Global Cyber Insurance Market—Gross Written Premiums 2015 to 2025



Sources: GlobalData and DBRS Morningstar.

What Is Cyber Insurance?

Cyber insurance, also known as cyber risk insurance or cyber liability insurance, is a relatively new specialty insurance product that helps protect organizations from the fallout of cyberattacks and hacking threats. A cyber insurance policy can help minimize business disruption during a cyber incident and its aftermath, as well as potentially cover the financial cost associated with a cyberattack. More technically, cyber insurance is a contract between an insurer and the insured (i.e., a company) to protect against losses that are related to computer- or network-based incidents.

Although cyber insurance policies have evolved over time, the most common coverage includes losses resulting from business interruption (e.g., lost revenue caused by systems being down), contingent business interruption (e.g., lost revenue caused by systems being down because of a third party's failure), digital asset destruction, data retrieval and system restoration costs, system failures, cyber extortion and ransomware, and breach response and remediation expenses, as well as network security and privacy liability. Nevertheless, cyber insurance coverage is still limited compared with the true amount of risk, and not all forms of cyber risk are covered by insurance. For instance, reputational costs that can be incurred following a cyberattack (including business revenues lost because of public perception of having poor cybersecurity) are typically noninsurable. Thus, most companies and organizations still have material exposure to the economic cost of cyberattacks, even when they purchase cyber insurance. According to IBM and the Ponemon Institute, the global average cost of a data breach in 2021 was $4.24 million, a 10% increase from 2019.[1]

Increases in Cyber Insurance Claims Continue to Drive Rates

Over the last two years, the cyber insurance market has experienced a significant surge in loss ratios and a corresponding deterioration in the profitability of cyber insurance products because of the rising frequency and severity of cyber insurance claims, particularly those related to ransomware.[2] For instance, according to the National Association of Insurance Commissioners, the combined ratio for stand-alone and package policies covering cyber risks in the United States jumped to 66.9% in 2020 from 44.6% in 2019.[3] This has caused cyber insurance rates in the U.S., the UK, and continental Europe to double during this period. Cyber insurers have reacted to the rise in ransomware losses not only by increasing rates but also by reducing available limits per policyholder, imposing higher deductibles, and cutting available capacity. DBRS Morningstar expects the hardening of cyber insurance rates to continue in 2022 given the potential fallout of the Russia-Ukraine conflict.

Additionally, similar to other insurance products potentially exposed to catastrophic losses, reinsurance and insurance companies are paying closer attention to the risk of a single cyber event affecting a large number of policyholders at the same time. Cyber risk has the potential to generate a chain of highly correlated losses because of the increasing connectivity of global communications and the widespread use of certain operating systems. A systemic event of such scale, particularly in the context of state and non-state actors employing cyber warfare against adversaries, has the potential to cost multiples of the estimated size of the current cyber market. These considerations have also supported the increase in cyber insurance rates as insurance companies incorporate

1. UpGuard, What is the Cost of a Data Breach in 2021?, February 23, 2022.
2. Ransomware is a type of malware that prevents or limits users from accessing their systems until a ransom is paid.
3. National Association of Insurance Commissioners, Report on the Cybersecurity Insurance Market, October 20, 2021.

catastrophe modelling in their pricing strategies, while some insurers have exited the cyber market altogether because of profitability concerns. Regulators are also increasingly worried about the potential systemic nature of cyber risks and have started to require additional capital to underwrite these products, which also contributes to rising cyber insurance rates. Finally, insurance and reinsurance companies are increasing cyber insurance rates to cover the additional costs of added services provided, such as negotiating with hackers and providing assistance for data recovery during ransomware attacks.

Attribution Will Be a Key Mitigant for Cyber Insurance Losses During Russia-Ukraine Conflict

Most property and casualty insurance products specifically exclude war, or only cover it in a very limited set of circumstances. Cyber insurance policies typically follow the same approach and do not cover cyber losses resulting from war or hostile acts. In practice, attributing cyberattacks to state actors, or their proxies, has proven to be extremely challenging because cyber warfare operations are typically not publicly acknowledged by the aggressor. Even in cases where a state actor can be strongly suspected of having caused a cyber incident, legal courts might not side with insurers, particularly if existing policy language is subject to interpretation. Recently, however, the New Jersey Superior Court ruled in favour of Merck & Co., Inc. (Merck), the U.S. pharmaceutical giant, which suffered losses of $1.4 billion in a NotPetya malware attack in 2017. At that time, the insurance claim was denied based on a war exclusion clause in Merck's policy. However, the New Jersey Superior Court decided that the war exclusion language was not applicable in this case as it could be interpreted to apply to "traditional" or kinetic war. A number of denied claims from the NotPetya attack are still going through courts to decide whether the suspected Russian cyberattack is covered or not based on the war exclusion clause.

Since 2019, insurers and reinsurers have reviewed and tightened war exclusion language in their cyber insurance policies as well as in their all-risk property policies that could include "silent cyber" coverage, which involves situations in which a policy does not explicitly include or exclude cyber risk. In November 2021, the Lloyd's of London market released four new exclusion clauses for cyber insurance policies that aim to clarify whether cyber war is covered. However, in DBRS Morningstar's opinion, attribution of cyber warfare remains a challenge because it places the onus on the insurer to demonstrate that a cyber incident was actually performed by a state actor or its proxy in the absence of official confirmation from intelligence agencies in the targeted country, which could take an impractical amount of time to obtain (this information may also never be disclosed for security reasons). Nevertheless, we expect that insurers and reinsurers will continue to clarify their cyber war exclusions to face the new realities of state-sponsored cyberattacks. Although cyber insurance claims are likely to increase for the European and North American insurance industry in the context of the Russia-Ukraine conflict, given the increasing sophistication of cyber insurance underwriting, reduced limits and capacity, and the relatively low participation of cyber insurance products in overall portfolios, losses resulting from cyber claims should remain manageable for our rated insurers and reinsurers.

Related Research

- *War, Weather, and Coronavirus Create Headwinds for Reinsurers Following Strong 2021 Results*, March 4, 2022.
- *Cost of December Tornado Outbreak Expected to Be Within Historical Range and Manageable for U.S. P&C Insurers*, December 15, 2021.
- *IFRS 17: A Significant Change for the Global Insurance Industry*, November 29, 2021.
- *The Global Supply Chain Crisis Exposes the Limits of Business Interruption Insurance*, November 2, 2021.
- *Global Reinsurers Post Record Earnings in H1 2021 but Face Headwinds from Catastrophe Losses and Coronavirus Litigation*, September 29, 2021.
- *The Suez Canal Blockage Is Likely to Have a Limited Impact on the Global Insurance Industry*, March 30, 2021.

Note:
All figures are in U.S. dollars unless otherwise noted.

About DBRS Morningstar

DBRS Morningstar is a full-service global credit ratings business with approximately 700 employees around the world. We're a market leader in Canada, and in multiple asset classes across the U.S. and Europe.

We rate more than 3,000 issuers and nearly 60,000 securities worldwide, providing independent credit ratings for financial institutions, corporate and sovereign entities, and structured finance products and instruments. Market innovators choose to work with us because of our agility, transparency, and tech-forward approach.

DBRS Morningstar is empowering investor success as the go-to source for independent credit ratings. And we are bringing transparency, responsiveness, and leading-edge technology to the industry.

That's why DBRS Morningstar is the next generation of credit ratings.

Learn more at dbrsmorningstar.com.